

EXHIBIT H

Mini Markman 30 Terms/Phrases to Address

1. Set forth below are the twelve claims designated for the “Mini-Markman” proceeding.
2. The parties, in accordance with the Court’s February 21, 2003, Order, have agreed to narrow the “Mini-Markman” proceeding to a selected thirty terms and phrases, set forth in boldface below.
3. Bold denotes the terms and the phrases that the parties have designated to be construed in the “Mini-Markman” proceeding; underscoring denotes the designation is a phrase.
4. Bolding of the claim number indicates that Microsoft construes the claim as a whole as requiring its “Global Construction” of “VDE.”

U.S. Patent No. 6,253,193

1. A method comprising:
receiving a digital file including music;
storing said digital file in a first **secure** memory of a first device;
storing information associated with said digital file in a **secure** database stored on said first device,
said information including at least one **budget control** and at least one **copy control**, said at
least one **budget control** including a budget specifying the number of copies which can be
made of said digital file; and said at least one copy control controlling the copies made of
said digital file;
determining whether said digital file may be **copied** and stored on a second device based on at least
said **copy control**;
if said **copy control** allows at least a portion of said digital file to be **copied** and stored on a second
device,
copying at least a portion of said digital file;
transferring at least a portion of said digital file to a second device including a memory and an
audio and/or video output;
storing said digital file in said memory of said second device; and
including playing said music through said audio output.

11. A method comprising:
receiving a digital file;
storing said digital file in a first **secure** memory of a first device;
storing information associated with said digital file in a **secure** database stored on said first device,
said information including a first **control**;
determining whether said digital file may be **copied** and stored on a second device based on said first
control,
said determining step including identifying said second device and determining whether said
first **control** allows transfer of said **copied** file to said second device,

said determination based at least in part on the features present at the device to which said **copied** file is to be transferred;
if said **first control** allows at least a portion of said digital file to be **copied** and stored on a second device,
 copying at least a portion of said digital file;
 transferring at least a portion of said digital file to a
 second device including a memory and an audio and/or video output;
 storing said digital file in said memory of said second device; and
 rendering said digital file through said output.

15. A method comprising:

receiving a digital file;

an **authentication** step comprising:

 accessing at least one **identifier** associated with a first device or with a user of said first device;
 and

 determining whether said **identifier** is associated with a device and/or user authorized to store said digital file;

storing said digital file in a first **secure** memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;

storing information associated with said digital file in a **secure** database stored on said first device, said information including at least one **control**;

determining whether said digital file may be **copied** and stored on a second device based on said at least one **control**;

if said at least one **control** allows at least a portion of said digital file to be **copied** and stored on a second device,

copying at least a portion of said digital file;

 transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

 storing said digital file in said memory of said second device; and
 rendering said digital file through said output.

19. A method comprising:

receiving a digital file at a first device;

establishing communication between said first device and a **clearinghouse** located at a location remote from said first device;

 said first device obtaining authorization information including a key from said **clearinghouse**;

 said first device using said authorization information to gain access to or make at least one **use** of said first digital file, including using said key to decrypt at least a portion of said first digital file; and

 receiving a first **control** from said **clearinghouse** at said first device;

storing said first digital file in a memory of said first device;

using said first **control** to determine whether said first digital file may be **copied** and stored on a second device;
if said first **control** allows at least a portion of said first digital file to be **copied** and stored on a second device,
copying at least a portion of said first digital file;
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;
storing said first digital file portion in said memory of said second device; and
rendering said first digital file portion through said output.

U.S. Patent No. 6,185,683

2. A system including:
a first apparatus including,
 user **controls**,
 a communications port,
 a processor,
 a memory storing:
 a first **secure container** containing a governed item, the first **secure container** governed item being at least in part encrypted; the first **secure container** having been received from a second apparatus;
 a first **secure container** rule at least in part governing an **aspect** of access to or **use** of said first **secure container** governed item, the first **secure container** rule, the first **secure container** rule having been received from a third apparatus different from said second apparatus; and
 hardware or software used for receiving and opening **secure containers**, said **secure containers** each including the capacity to **contain** a governed item, a **secure container** rule being associated with each of said **secure containers**;
a **protected processing environment** at least in part protecting information **contained** in said **protected processing environment** from tampering by a user of said first apparatus, said **protected processing environment** including hardware or software used for applying said first **secure container** rule and a second **secure container** rule in combination to at least in part govern at least one **aspect** of access to or **use** of a governed item **contained** in a **secure container**; and
hardware or software used for transmission of **secure containers** to other apparatuses or for the receipt of **secure containers** from other apparatuses.

U.S. Patent No. 6,157,721

1. A security method comprising:
(a) **digitally signing** a first load module with a first **digital signature** designating the first load module for **use** by a first **device class**;

- (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class;
- (c) distributing the first load module for use by at least one device in the first device class; and
- (d) distributing the second load module for use by at least one device in the second device class.

34. A protected processing environment comprising:

- a first **tamper resistant barrier** having a first security level,
- a first **secure execution space**, and
- at least one arrangement within the first **tamper resistant barrier** that prevents the first **secure execution space** from executing the same **executable** accessed by a second **secure execution space** having a second **tamper resistant barrier** with a second security level different from the first security level.

U.S. Patent No. 5,920,861

- 58. A method of creating a first secure container**, said method including the following steps;
- accessing a descriptive data structure, said descriptive data structure including or addressing organization information at least in part describing a required or desired organization of a content section of said first **secure container**, and
- metadata information at least in part specifying at least one step required or desired in creation of said first **secure container**;
- using said descriptive data structure to organize said first **secure container** contents;
- using said metadata information to at least in part determine specific information required to be included in said first **secure container** contents; and
- generating or identifying at least one rule designed to **control** at least one **aspect** of access to or use of at least a portion of said first **secure container** contents.

U.S. Patent No. 5,982,891

- 1. A method for using at least one resource processed in a secure operating environment at a first appliance**, said method comprising:
- securely receiving a first entity's control** at said first appliance, said first entity being located remotely from said operating environment and said first appliance;
- securely receiving a second entity's control** at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and
- securely processing a data item at said first appliance**, using at least one resource, including **securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item.**

U.S. Patent No. 5,892,900

155. A virtual distribution environment comprising
a first **host processing environment** comprising
a central processing unit;
main memory operatively connected to said central processing unit;
mass storage operatively connected to said central processing unit and said main memory;
said mass storage storing tamper resistant software designed to be loaded into said main memory and
executed by said central processing unit, said tamper resistant software comprising:
machine check programming which derives information from one or more aspects of said host
processing environment,
one or more storage locations storing said information;
integrity programming which causes said machine check programming to **derive** said information,
compares said information to information previously stored in said one or more storage
locations, and
generates an indication based on the result of said **comparison**; and
programming which takes one or more actions based on the state of said indication;
said one or more actions including at least temporarily halting further processing.

U.S. Patent No. 5,917,912

8. A process comprising the following steps:
accessing a first record **containing** information directly or indirectly identifying one or more elements
of a first **component assembly**,
at least one of said elements including at least some **executable programming**,
at least one of said elements constituting a load module,
said load module including **executable programming** and a header;
said header including an execution space **identifier** identifying at least one aspect of an
execution space required for use and/or execution of the load module associated
with said header;
said execution space **identifier** provides the capability for distinguishing between
execution spaces providing a higher level of security and execution spaces
providing a lower level of security;
using said information to identify and locate said one or more elements;
accessing said located one or more elements;
securely assembling said one or more elements to form at least a portion of said first **component
assembly**;
executing at least some of said **executable programming**; and
checking said record for validity prior to performing said executing step.

35. A process comprising the following steps:
at a first processing environment receiving a first record from a second processing environment remote
from said first processing environment;

said first record being received in a **secure container**;
said first record **containing** identification information directly or indirectly identifying one or more elements of a first **component assembly**;
at least one of said elements including at least some **executable programming**;
said **component assembly** allowing access to or use of specified information;
said **secure container** also including a first of said elements;
accessing said first record;
using said identification information to identify and locate said one or more elements;
said locating step including locating a second of said elements at a third processing environment located remotely from said first processing environment and said second processing environment;
accessing said located one or more elements;
said element accessing step including retrieving said second element from said third processing environment;
securely assembling said one or more elements to form at least a portion of said first **component assembly** specified by said first record; and
executing at least some of said **executable programming**,
said executing step taking place at said first processing environment.